Security must be part of the IoT project's design phase, not an afterthought. For example, strong passwords, multi-factor authentication, and data encryption should all be standard. These measures prevent the threat of stolen credentials or eavesdropping through man-in-the-middle attacks. In addition, mobile IoT networks, such as LTE-M and NB-IoT, offer secure communication channels that are particularly useful for IoT deployments in mission-critical applications.

"If you see a [project] specification that doesn't mention security, then it's a bad sign," states Greg Turner, senior director of engineering at Honeywell.

Businesses should adopt management platforms that provide visibility into every IoT device connected to a corporate network, complete with the ability to issue updates to firmware and software that can patch known vulnerabilities.

Part of the IoT security challenge is that vendors often lack frameworks for providing ongoing updates. But governments are increasingly aware of the importance of IoT and digital technologies to the economy and national security. As a result, many have introduced or are planning legislation to place manufacturers' obligations to adhere to specific standards.

"Manufacturers are building these embedded security technology practices into the hardware and software of their IoT devices," Kevin Curran, a senior member of IEEE and professor of cyber security at Ulster University, told AI Business. "Unfortunately, there are simply far too many older IoT devices which are unable to be updated to support these policies in their software. An intermediate firewall needs to be added to the network to defend those devices against outside attacks. However, firewalls only prevent a subset of attacks; other problems such as eavesdropping require additional mechanisms in place."

Solving the IoT security challenge will require action from legislators, businesses, and individuals. In the current economic climate, it is understandable that the focus for many enterprises is on survival, and the IoT offers a path to recovery. But unless organizations address the security challenge, they could face a very different threat to their existence.